UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

COTTON PATCH CAFE, INC.,	)	
	)	
Plaintiff,	)	**CIVIL ACTION NO. 1:09-cv-03242-MJG**
	)	
v.	)	
	)	
MICROS SYSTEMS, INC.,	)	**SECOND AMENDED ORIGINAL**
	)	**COMPLAINT AND DEMAND FOR**
	)	**JURY TRIAL**
Defendant.	)	

Plaintiff Cotton Patch Cafe, Inc. ("Plaintiff"), by and through undersigned counsel, and for its Second Amended Original Complaint against Defendant Micros Systems, Inc. ("Defendant" or "Micros"), respectfully states as follows:

JURISDICTION AND VENUE

1. This Court has jurisdiction over this matter pursuant to 28 U.S.C. § 1332(a) because the parties to the action are citizens of different states and the amount in controversy exceeds the sum or value of $75,000, exclusive of interest and costs.

2. Venue is proper in this district pursuant to 28 U.S.C. § 1391(a)(1) because the defendant, for venue purposes, resides in this district.

THE PARTIES

3. Plaintiff Cotton Patch Cafe, Inc. is a Texas corporation with its principal place of business located at 600 East Dallas Road, Suite 300, Grapevine, Texas 76051.

4. Defendant Micros Systems, Inc. is a Maryland corporation located at 7031 Columbia Gateway Drive, Columbia, Maryland 21046 that can be served pursuant to Fed. R. Civ. P. 5.

FACTUAL BACKGROUND

5. Plaintiff owns and operates a restaurant chain with locations in Texas and New Mexico. One of Plaintiff's restaurants is located in Nacogdoches, Texas. This location serves as a popular eating establishment for local residents and is the source of the facts and circumstances giving rise to this lawsuit.

6. In 2001, Defendant, a recognized leader in the hospitality industry, induced Plaintiff to undertake a project in which Defendant sold, set up, and later began servicing a point-of-sale system for processing credit card transactions for Plaintiff's Nacogdoches location (the "Restaurant") (collectively the "Project"). The system eventually installed and maintained pursuant to the Project consists of hardware and software originally installed and later serviced and supported by Defendant to process point of sale transactions at the Restaurant. Like many restaurant operators, Plaintiff uses a credit card processing system for the convenience of its customers at the Restaurant. The system allows customers to pay for meals using either credit or debit cards. The system is similar to card processing systems found at other restaurants and establishments that allow customers to pay for products and services using a credit or debit card. At no time during the Project was Plaintiff given any responsibility or direction for the security of the system hardware or software. In fact, Defendant explicitly instructed Plaintiff not to tamper with, maintain, or service the system in any way, but required that the system be maintained under its control and direction. Plaintiff purchased services from Defendant as needed with respect to the operation of the system. Those services were not documented by written contract and were all a part of the Project. Defendant was aware that Plaintiff relied upon Defendant for the service and maintenance of the system, and encouraged that reliance.

Plaintiff's claims are limited to only a small number of specific transactions making up the Project.

7. In 2004, the card processing system in question was subject to federal statutory standards and broadly accepted payment card industry data security standards imposed by the major credit card companies and related financial institutions. The standards set forth the requirements for point of sale systems, including requirements for protecting cardholder data, developing and maintaining secure systems and applications, restricting access to cardholder data, tracking and monitoring access to network resources and cardholder data, and regularly testing security systems and processes. Despite regularly providing services to the system and encouraging Plaintiff's reliance, Defendant never advised Plaintiff that the system was not compliant with these statutes and standards even though Defendant was aware that the system was not compliant. Furthermore, beginning in or around 2006, when Plaintiff inquired about the system's compliance with these uniform standards, Defendant represented to Plaintiff that the system utilized by Plaintiff complied or would be made to comply with all standards and particularly with respect to credit card data storage and encryption. Indeed, Defendant provided services purportedly to inspect and upgrade the system and produced purported "evidence" that the system was secure and met the required security standards. Defendant continued to maintain complete control of the system, even replacing a server, continued regular service and maintenance of the system, and continued to fail to advise Plaintiff that the system was not compliant with prevailing standards. This conduct occurred even though Plaintiff's use of a non-compliant system subjected it to possible fines from credit card companies and exposure to theft of its customers' credit card data. Such conduct also occurred even though Defendant was aware of data breaches victimizing other customers with the same type of point of sale system and

ongoing criminal investigations involving these systems.

8. Beginning as early as 2006 and in major part during May and June, 2007, and unbeknownst to Plaintiff, unknown third-parties began illegally accessing the Micros card processing system at Plaintiff's Restaurant, stealing Plaintiff's customers' credit card data, including full track data (which, contrary to Defendant's representations, were actually stored and transmitted unencrypted and unsecured on and from the system in violation of security standards) and making fraudulent charges on the customers' card accounts. Plaintiff did not become aware of the breach and subsequent thefts until August 23, 2007, when RBS Lynk, a leading payment processing company, alerted Plaintiff that Visa's and MasterCard's fraud departments had observed fraudulent transactions that suggested Plaintiff's Restaurant was the common point of purchase where cardholder data may have been compromised.

9. Despite its representations to the contrary and failures to disclose, Defendant failed to provide compliant Micros software, a compliant firewall, antivirus software updates for the system, non-default or non-common passwords, and failed to encrypt and remove credit card data in accord with industry standards broadly adopted no later than 2004. Had the firewall, antivirus software updates, proper passwords, encryption and removal of credit card data been provided as represented, the illegal access and theft would not have occurred. Defendant failed to ensure, despite its representations to the contrary, that its services complied with relevant industry security standards including those accepted and publicized as late as in 2004. Furthermore, Defendant knew software it sold with the system server was non-compliant with prevailing standards and made direct misrepresentations that its software was compliant, all pursuant to an elaborate ruse based upon communications from Visa. Successful exploitation of the system's failure to meet standards despite the services provided could, and did, result in

remote access of cardholder data by third parties and subjected Plaintiff to charges and fines from credit card companies and related financial institutions.

10. In March 2006, Defendant sold to Plaintiff a new server and upgraded software (collectively, the "Server") for use at Plaintiff's Nacogdoches restaurant. Due to a known and pervasive failure to train its employees, a system server was installed with malware already placed on the system and configured to store full track data in system page files, all in violation of known standards. As discussed in the preceding paragraph, Defendant was aware that the Server failed to comply with relevant industry data security standards, but failed to notify Plaintiff of that important fact. Moreover, the Server provided by Defendant was infected with malware prior to installation at Plaintiff's Nacogdoches restaurant. The malware provided the necessary means for an attacker to take control of the Server, install additional malware, identify customer credit card data (including full track data), and exfiltrate that data. Plaintiff was unaware that the Server was delivered with malware already installed on it, and Defendant failed to notify Plaintiff of the malware or prevent its installation. In addition, the Server was designed by Defendant to store data, including unencrypted full track data, in "page files" that could be accessed by an attacker using the pre-installed malware. The presence of pre-installed malware and the storage of full track data in page files comprised serious flaws in the Server and directly contributed to the data security breach at Plaintiff's Nacogdoches restaurant.

11. Defendant knew or should have known of the system's failure to meet payment card industry standards despite the services provided and was aware of the potential for harm for system users, as other businesses using similar Micros systems had experienced cardholder data thefts. After the broad adoption of the uniform payment card industry standards in 2004, Defendant represented to Plaintiff that the system would be serviced, supported, and monitored

by Defendant via remote access and otherwise in order to comply with these standards as well as prior existing security standards. At that time, Defendant further represented that, as a result of the services, the system was state of the art, was sufficient for Plaintiff's needs, and would protect Plaintiff's business. Defendant made numerous other representations to Plaintiff regarding the viability, safety, and security that its services made to the system in light of then prevailing standards. None of Defendant's representations were true. Furthermore, Defendant deceptively failed to disclose information regarding Plaintiff's non-compliant system (including stored malware), lack of training, and other customer data breaches involving the same or similar system in order to induce Plaintiff into transactions for goods and services that were non-compliant and damaging to it which were a part of the Project.

12. As a result of Defendant's conduct, Plaintiff has suffered damages in excess of the Court's jurisdictional minimum.

PERFORMANCE AND CONDITIONS PRECEDENT

13. All conditions precedent to the bringing of this lawsuit have been performed, excused, waived, or otherwise satisfied.

14. To the extent necessary, Plaintiff pleads the discovery rule.

COUNT ONE - VIOLATIONS OF THE TEXAS DECEPTIVE TRADE PRACTICES ACT

15. Plaintiff re-alleges and incorporates by reference all facts and allegations set forth in Paragraphs 1-13.

16. Plaintiff is a consumer, as defined under § 17.45(4) of the Texas Business and Commerce Code. Plaintiff is entitled to bring claims arising from specific transactions making up the Project as the total consideration expended in relation to the transactions at issue in the Project was less than $500,000.00.

17. Defendant violated the Texas Deceptive Trade Practices Act ("DTPA") and acted to Plaintiff's detriment by taking advantage of Plaintiff's lack of knowledge, ability, experience, or capacity to a grossly unfair degree, which constitutes an "unconscionable action or course of action" pursuant to § 17.45(5) of the Texas Business and Commerce Code. Plaintiff had no knowledge or experience with payment card industry standards and securing card processing systems and customer data. In addition, Plaintiff had no knowledge regarding the coding and programming of the Micros system, including whether the system was designed to be PCI complaint. Beginning no later than 2006, Defendant stated and continued to reassure Plaintiff that Defendant would ensure that payment card industry standards concerning security of customer data would be met and were in fact met. Defendant's statements were untrue. Defendant further acted deceptively in failing to disclose Plaintiff's non-compliance and ongoing criminal investigations involving the failures of its products.

18. Defendant further violated the DTPA § 17.46(b) by committing false, misleading, or deceptive acts or practices including: (i) causing confusion or misunderstanding to Plaintiff about the approval or certification of the services and goods provided; (ii) causing confusion or misunderstanding as to certification by another; (iii) representing that the goods and services had characteristics, uses, and benefits that they did not; (iv) representing that the goods and services were of a particular standard, quality, or grade when they were not; (v) representing that work or services had been performed on, or parts replaced in, goods when the work or services were not performed; and (vi) failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

19. Defendant's DTPA violations were a producing cause of Plaintiff's damages, which exceed the Court's minimum jurisdictional limits. Moreover, Defendant's violations were committed intentionally and/or knowingly, and therefore Plaintiff is entitled to treble damages under the DTPA. Plaintiff also is entitled to recover reasonable attorneys' fees under the DTPA and litigation costs and expenses including expert witness fees.

COUNT TWO – NEGLIGENCE

20. Plaintiff re-alleges and incorporates by reference all facts and allegations set forth in Paragraphs 1-18.

21. Defendant negligently serviced the system at the Restaurant. Defendant had a duty to service the system with care, skill, and reasonable expedience in light of prevailing standards. Defendant also negligently provided a defective server for use at Cotton Patch's Nacogdoches restaurant because, inter alia, the server was infected with malware and stored full track data. Defendant's negligent affirmative conduct proximately caused Plaintiff's damages. As a result of Defendant's wrongful conduct, Plaintiff has been damaged in an amount that exceeds this Court's jurisdictional minimum. Plaintiff now sues and seeks actual and exemplary damages.

COUNT THREE – NEGLIGENT MISREPRESENTATION

22. Plaintiff re-alleges and incorporates by reference all facts and allegations set forth in Paragraphs 1-20.

23. Defendant made representations to Plaintiff in the course of its business. Defendant supplied false information to Plaintiff for its guidance. Defendant did not exercise reasonable care or competence in obtaining or communicating the information. Plaintiff justifiably and substantially relied on Defendant's representations to its detriment. Plaintiff has suffered damages as a result of the Defendant's negligent misrepresentations.

24. As a result of Defendant's wrongful conduct, Plaintiff has been damaged in an amount that exceeds this Court's jurisdictional minimum. Plaintiff now sues and seeks actual and exemplary damages.

COUNT FOUR – GROSS NEGLIGENCE

25. Plaintiff re-alleges and incorporates by reference all facts and allegations set forth in Paragraphs 1-23.

26. Defendant's conduct constitutes gross negligence in that its conduct involved an extreme degree of risk, considering the probability and magnitude of the potential harm to Plaintiff, and Defendant had actual, subjective awareness of the risk involved but proceeded with conscious indifference to the rights, safety, and welfare of Plaintiff and its customers. As a result, Plaintiff is entitled to exemplary damages.

COUNT FIVE – FRAUD BY NONDISCLOSURE

27. Plaintiff re-alleges and incorporates by reference all facts and allegations set forth in Paragraphs 1-25.

28. Defendant concealed from or failed to disclose to Plaintiff that the system was unprotected and did not comply with applicable data security standards, the software on the server that Defendant sold to and installed for Plaintiff in 2006 did not comply with applicable data security standards, Plaintiff would be subjected to fines from credit card companies because the system was non-compliant, compliant software for the system was available or would be available in the near future, and even though customer card data was being masked, the system was storing the data when it should not have been. Defendant also failed to disclose that its personnel were not trained on compliance issues and were not competent in compliance issues.

29. Defendant had a duty to disclose these facts because Defendant represented to Plaintiff that Defendant would protect, and was protecting, the system and would ensure, and was ensuring, that the system complied with applicable data security standards. These facts were material and important to Plaintiff, as Plaintiff relied on and paid Defendant to ensure the system was fully compliant and was protecting customer card data. If Plaintiff had known the system was non-compliant and Defendant personnel were not trained, Plaintiff would have taken other measures to ensure the system became compliant, including but not limited to contracting with a competitor of Defendant.

30. Defendant knew Plaintiff was ignorant of, and did not have an equal opportunity to discover, these facts. Not only did Plaintiff retain Defendant to protect the system and ensure the system complied with applicable data security standards because Defendant, not Plaintiff, has the expertise to ensure the system was compliant, but Defendant instructed Plaintiff not to tamper with the system in any way and to let Defendant handle all system modifications, upgrades, and changes. Defendant, however, was deliberately silent when it had a duty to speak, and Defendant intended Plaintiff to rely on Defendant's omissions and concealment and refrain from moving Plaintiff's business to one of Defendant's competitors. Plaintiff relied on Defendant's omissions and concealment by not pursuing other ways and means of protecting the system and ensuring it was compliant with applicable data security standards. Defendant's omissions and concealment caused Plaintiff's injury because if Plaintiff had known the system was not compliant and not protected, Plaintiff would have taken whatever measures were necessary to do so and thereby would have been able to prevent the loss.

PRAYER

WHEREFORE, Plaintiff requests that Defendant be cited to appear and answer herein,

and that upon final hearing or trial of this cause, Plaintiff be granted judgment against Defendant for the following:

a. Actual damages;

b. Consequential damages including loss of goodwill and lost profits;

c. Treble damages;

d. Exemplary damages;

e. Reasonable and necessary attorneys' fees pursuant to Texas Business & Commerce Code § 17.50(d) and as otherwise allowed by law;

f. Pre- and post-judgment interest at the highest lawful rate;

g. Costs of suit and litigation expenses including expert witness fees; and

h. Such other and further relief, both general and special, at law and in equity, to which Plaintiff justly may be entitled.

Respectfully submitted,

KANE RUSSELL COLEMAN & LOGAN, P.C.

/s/ Robert N. LeMay
Robert N. LeMay (Admitted pro hac vice)
3700 Thanksgiving Tower
1601 Elm Street
Dallas, Texas 75201
Tel: (214) 777-4200
Fax: (214) 777-4299

Craig D. Roswell
Federal Bar No. 433406
NILES, BARTON & WILMER, LLP
111 South Calvert Street, Suite 1400
Baltimore, MD 21202
Tel: (410) 783-6341
Fax: (410) 783-6486

ATTORNEYS FOR PLAINTIFF COTTON PATCH CAFE, INC.

CERTIFICATE OF SERVICE

This is to certify that on _____, 2011, I caused the foregoing document to be filed electronically with the Clerk of Court through ECF, and that ECF did send an e-notice of the electronic filing to the following:

Steven A. Allen
Hodes, Pessin & Katz, P.A.
901 Dulaney Valley Road, Ste. 400
Towson, Maryland 21204

Ryan Bangert
Baker Botts LLP
2001 Ross Avenue, Ste. 600
Dallas, Texas 75201

/s/ Robert N. LeMay
Robert N. LeMay